

Original citation:

Mäses, Sten, Hallaq, Bilal and Maennel, Olaf (2017) Obtaining better metrics for complex serious games within virtualised simulation environments. In: 11th European Conference on Games Based Learning, Graz, Austria, 5-6 Oct 2017. Published in: Proceedings of 11th European Conference on Games Based Learning

Permanent WRAP URL:

<http://wrap.warwick.ac.uk/94296>

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions. Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher's statement:

Published version: http://www.academic-bookshop.com/ourshop/prod_6222013-ECGBL-2017-PDF-The-11th-European-Conference-on-GameBased-Learning.html

A note on versions:

The version presented here may differ from the published version or, version of record, if you wish to cite this item you are advised to consult the publisher's version. Please see the 'permanent WRAP URL' above for details on accessing the published version and note that access may require a subscription.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

Obtaining Better Metrics for Complex Serious Games Within Virtualised Simulation Environments

Sten Mäses¹, Bil Hallaq², Olaf Maennel¹

¹Department of Software Science, Tallinn University of Technology, Estonia

²Cyber Security Department, WMG - University of Warwick, U.K.

sten.mases@ttu.ee

bh@warwick.ac.uk

olaf.maennel@ttu.ee

Abstract: Recent technological advancements are providing significant results in enriching learning through serious games in the field of information and communication technology (ICT). One such advancement is the ability to create highly complex virtualised environments that realistically simulate organisations' ICT systems, enabling participants to develop practical hands-on skills in a controlled environment. During such exercises, a critical component is the ability to track individual participants progress. This requires an evaluation system to be in place. Within traditional computer gaming environments, it is relatively easy to automate the tracking and capture of a specific player's moves, clicks and other interaction. Within simulations of serious games such as those used for training defence and attack mitigation techniques in a computer network, tracking such activities in an automated manner is significantly more complex. Using serious games in the field of cybersecurity as an example, we provide in this work a mapping of different types of metrics for serious games run within virtual lab environments and suggest various ways in which they can be measured. This work will assist serious game designers, developers, organisers and assessors obtain a greater understanding of the state of the art possibilities for measuring the performance of participants. It will also enable researchers to build a solid foundation in which they can develop new approaches for more efficient learning through virtualized simulations.

Keywords: serious games analytics, game-based learning, cybersecurity, computer simulation environments

1. Introduction

Cybersecurity is one of the fields that faces an ongoing global resource crisis (Loeb, 2015). Due to the lack of qualified personnel in this rapidly growing field, it is increasing difficult to find technically proficient individuals (Evans, K. & Reeder, 2010). Like in other fields, a qualified cybersecurity specialist needs sufficient knowledge together with practical skills (Assante and Tobey, 2011). Knowledge acts as an enabler for different skills, and skills can be directly applied to solve everyday tasks and problems. Obtaining the relevant skills though, especially in complex areas such as Cybersecurity is often not a simple task to be achieved. As with many fields, it is risky to let inexperienced people to access systems in order to learn (Lateef, 2010). Therefore, various educational simulations have been developed to address this issue.

Games such as chess and Go have been used for centuries to train strategical thinking, but the skills learnt from these games usually cannot be transferred straight to the real world. For example, while experience of chess can be inspirational for configuring a firewall, it is surely not sufficient. The big question with simulations is always, up to what extent are the skills learnt from the simulation transferrable to a real-life situation? In that perspective, the field of computer science has a significant advantage. Due to the popularity of cloud based systems, most technical skills needed from an IT specialist are connected to virtualised environments. Therefore, it is possible to create virtualised simulation environments that are almost or in some scenarios, identical to real-life systems.

The term serious games is often used in order to describe games with a non-entertaining purpose (Djaouti, Alvarez and Jessel, 2011). In this work, we take the cybersecurity field as an example and show how serious games can help us develop and measure relevant skills. For skill classification, we use Bloom's taxonomy (Starr *et al.*, 2008).

2. Related work

The concept of using digital games to support learning is not new. For more than a decade, many researchers have published numerous essays, articles and books on the topic of digital game-based learning (Eck, 2006). This research is largely motivated by the need to create more engaging learning environments. The educational effects of many simulations have also been researched quite widely throughout diverse fields such as flight simulators (Hays *et al.*, 1992), nursing (Jacobs, Beyer and Carter, 2017), and cybersecurity (Furfaro *et al.*, 2017).

There are also multiple serious games in the cybersecurity field that are used for the training of specialists. Tabletop exercises can be used to demonstrate the interrelationships of the technical, procedural and human aspects of cybersecurity (Ottis, 2014). In addition to these are numerous complex technical exercises designed to train security experts who protect critical IT systems such as Locked Shields (NATO CCDCOE, 2017), CYRAN (Hallaq *et al.*, 2016), U.S. Service Academies Cyber Defence Exercise (Carlin and Manson, 2011), and Cyber Shield (Henshel *et al.*, 2016).

In addition to the complex large-scale technical exercises there has been an increasing number of smaller scale exercises using virtualised simulation environments for different educational goals. Some are more general (Cano *et al.*, 2016) and others more specific, e.g. a lab for learning the concepts connected to denial of service (Ledford, Mountroudou and Li, 2016) or assessment of cybersecurity issues in Internet of Things (IoT) scenarios (Furfaro *et al.*, 2017). There are also both commercial (Buttyán, Félegyházi and Pék, 2016) and open source platforms (Ernits, Tammekänd and Maennel, 2015) for managing virtualised simulation environments.

Serious games which are run within virtualised simulation environments appear to be the best solution to ensure resilient, efficient and scalable cybersecurity exercises. They consist of different virtual machines (VM-s) that are interconnected to one or many networks. Similar technology is being used in large scale production environments for offering a diverse selection of cloud-based services – therefore the skills learnt from VM-based lab environments are highly applicable also outside of the lab.

Within this section we have reviewed various simulation environments and the complexities associated with them. While many projects are benefitting from the advantages of VM-based simulation environments, there is a lack of systematic approach to identify general guidelines for performance measurement of the participants of such exercises. Much of the work in this area typically happens in isolation and those that are federated or openly available, such as DETERLab (Wroclawski *et al.*, 2016), are not more widely adopted.

On the other hand, there is a growing body of literature on the topic of Serious Games Analytics (SEGA), but there is a shortage of research considering applying SEGA to VM-based simulation environments. This paper aims to clarify and structure some core concepts regarding SEGA in VM-based simulation environments. Within the next section we identify the types of virtual environments available and the benefits and drawbacks of each.

3. VM-based environments

VM-based environments can be divided based on the user's access level to the system.

In case of restricted access, the user has only predefined operations to choose from. This way the VM-based environment can stay on the background and provide the user with a simple user interface that is convenient for people with less technical skills. While it can be a good starting point for a deeper technical understanding, it is more focused on the first two levels of Bloom's taxonomy (Starr *et al.*, 2008), recall and comprehension.

In case of full access to the virtual machine, the user can choose their own methods and tools for tackling the task. This option is very realistic; therefore, it can be used for learning skills from all levels of Bloom's taxonomy. At the same time, it can be overwhelming for users with less technical skills. Also, it demands relatively high-throughput bandwidth in the case of doing the simulation remotely.

There are also options with selected access where the user can write their own commands through the browser interface, but the full graphical interface of the virtual machine is hidden. This approach can be considered as a compromise. All skill levels of the Bloom's taxonomy can still be reached, but the simulation is less realistic than in the case of full access to the virtual machine, because the user interface is likely slightly modified based on the simulation environment (e.g. browser constraints).

4. Performance metrics

Serious games are designed to support knowledge acquisition and/or skill development (Loh and Yanyan Sheng, 2013). Therefore, it is essential to assess the performance of the players. The performance is usually characterised by a score, that is comparable between the participants of the same serious game (Loh, Sheng and Ifenthaler, 2015). The input for the score comes from different measurement points. As different measurement points often measure similar metrics, then it is reasonable to form categories that encompass similar measurement points as illustrated in the **Figure 1**. To calculate the total score S_{total} , the input from different measurement points can be weighed as follows:

$$S_{total} = \frac{\sum_{i=1}^n w_i x_i}{\sum_{i=1}^n w_i}$$

where w_i is the weight and x_i is the performance metric value from one measurement point. Similarly, different weights can be assigned to different categories to prioritise some of them over the others.

As an example, let us imagine a cybersecurity-related serious game with the following two performance metric categories: availability of services and incident reporting. If the goal of this serious game is to promote the importance of proper incident reporting, then the weight of the according category can be several times higher than the weight of the other categories (in the current example, the availability of services). That way, the participants are encouraged to focus more on incident reporting and less on the availability of services. Of course, this kind of prioritisation only works if the participants are at least to some extent aware of the scoring system, not in case of a stealth assessment (DeRosier, Craig and Sanchez, 2012).

The weight for any performance metric is highly dependable on the game and should be fine-tuned during the testing phase based on the real results.

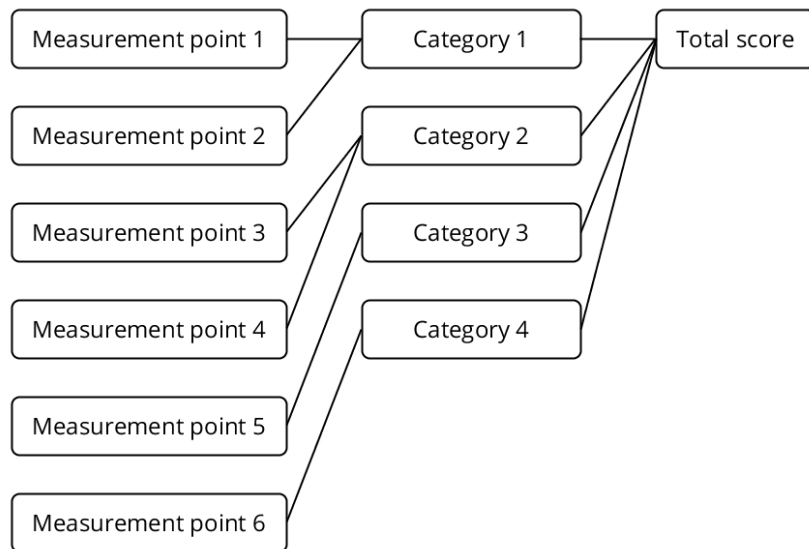


Figure 1: Categorising performance metrics

The total score is necessary in the case where the VM-based serious game is used for a competition or formal assessment and a final ranking list is required. A further analysis by performance metric categories (and potentially sub-categories) can provide much more valuable insights about the strengths and weaknesses of the participant (or participating team).

Each measurement point contributes to the final scoring of the serious game by measuring a specific metric.

Some metrics are measuring whether the main objective of a task was completed, while others give additional information about the way the participant achieved (or did not achieve) the required objective. The completion of a task can be measured in a binary (pass/fail) or continuous scale. Any continuous scale measurement can be turned into a binary measurement by introducing a threshold (e.g. defining the border between fail and pass).

Those metrics can be measured in various ways. In the following list, there are some of the commonly used metrics to consider.

4.1 Direct input

The objective of a VM-based serious game participant can be to find some specific information using the virtual machines and then report this information to be evaluated. Reporting can be done through a side-channel, such as a Moodle platform¹ that the user can access outside of the virtual machines. For example, an ICT security project DECAMP in Munich (Alexandru Soceanu, Maksym Vasylenko and Alexandru Gradinaru, 2017) developed a lab based on Moodle education platform interfaced with OpenStack² cloud computing platform.

Using the metrics based on direct input is more reliable if the objectives are slightly customised for each participant. For example, the task for each participant can be to decrypt a message, but the content of the message to be submitted for evaluation could be different for each participant. This way, it can be confirmed, that no participant reached the result by simply getting the required information from others.

4.2 Automated scoring script

Checking the objectives of the VM-based serious game can be automated. For example, an automated script can evaluate the uptime of a service or check the contents of a specific configuration file. When using automated scoring, it is important to limit the participant's access to the scoring script. For example, if the scoring script resides in the same virtual machine which the user has full access to, then it is not difficult to alter the scoring script. Therefore, it would be possible for a person to get maximum points without even completing the actual given objective.

To protect the integrity of the scoring system, it is possible to place the scoring script into another virtual machine (that the user has no access to), or to protect the scoring script by limiting the user administrative rights.

4.3 Time

Time spent on VM-based serious game objectives can give valuable insights about the participant's abilities. Average time spent on every task can give a good basis for further analysis. In addition, it can be used as a trigger for displaying hints to participants who have gotten stuck in a pre-defined scenario.

It should be considered though, that the time spent on different tasks can be influenced by many external factors, e.g. user's hardware, Internet bandwidth, coffee breaks etc.

Also, while usually a faster task completion indicates a more skilled participant, it should be considered that unrealistically fast times might indicate a fault in the system or a malicious participant instead.

4.4 String similarity metrics

Comparing unknown performance against known experts can be done using string similarity metrics such as Levenshtein distance (Loh and Sheng, 2015). String similarity metrics can be used to compare activity logs, e.g. history of typed commands by the participant. This allows to evaluate the efficiency of the participant's actions.

4.5 Tools

In VM-based simulation, the user often has full control over the machine and therefore also freedom to choose amongst multiple tools. The choice of a specific software (e.g. Nmap³) or a programming language (e.g. Bash or Python) can give extra information about the participant's skillset.

¹ Moodle, <https://moodle.com>

² OpenStack Project, <http://www.openstack.org>

³ Nmap Security Scanner, <https://nmap.org>

5. Mapping of skills

Measurements are meaningless unless they are connected to specific skills. Therefore, it is needed to define the particular skillset that the serious game should develop and measure. NICE Cybersecurity Workforce Framework (Newhouse *et al.*, 2016) could be used as a reference for mapping relevant cybersecurity skills. For ICT occupations in general, the e-Skills Match framework (Fernández-Sanz, Gómez-Pérez and Castillo-Martínez, 2017) can be used for integrating the existing ICT related reference schemes and standards. Using widely established standards and frameworks as a basis, helps to compare the performance metrics across different systems and organisations.

Skill differentiation is also important. Technological advances enable us to keep track of more data and that enables more granular tracking of performance and abilities (Umbleja *et al.*, 2014). With the help of automated scoring systems, it is possible to give individual and highly specific feedback for each participant of a virtual simulation. **Figure 2** shows how skills can be linked to different performance measurement categories. Additionally, different granular skills can be grouped together as skill sets. This provides a high-level overview of a participant's skills and can be easily communicated. For example, it would be confusing for a job ad to specify hundreds of granular skills that are required for a position. Instead a wider skill set is often described. If the same skill set is defined based on a VM-based serious game skills and linked to measurements, then it is possible to have an automated and scalable system that can quickly find the job applicant with the most fitting technical skill sets.

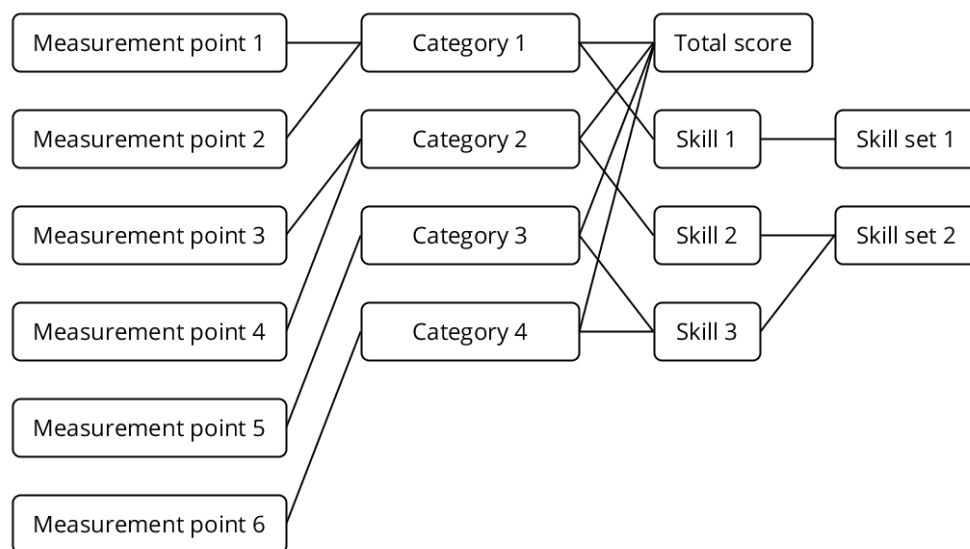


Figure 2: Categorised performance metrics linked to skills

In the current example (**Figure 2**), the total score is not affected by the skill sets. The scores for each skill set help to give participants detailed and individual feedback. In a different context, a total score can be also based on the similarity to the pre-defined skill sets (e.g. when finding the job applicant with best fitting technical background). It is important to note that there can be various types of connections between measurement points, categories, skills and skill sets. For example, there can be many measurement points giving input to a common category. Similarly, many categories of performance metrics can be connected to one skill (or one skill to many categories). **Figure 3** provides an example for using the described framework for mapping the performance metrics and relevant skills.

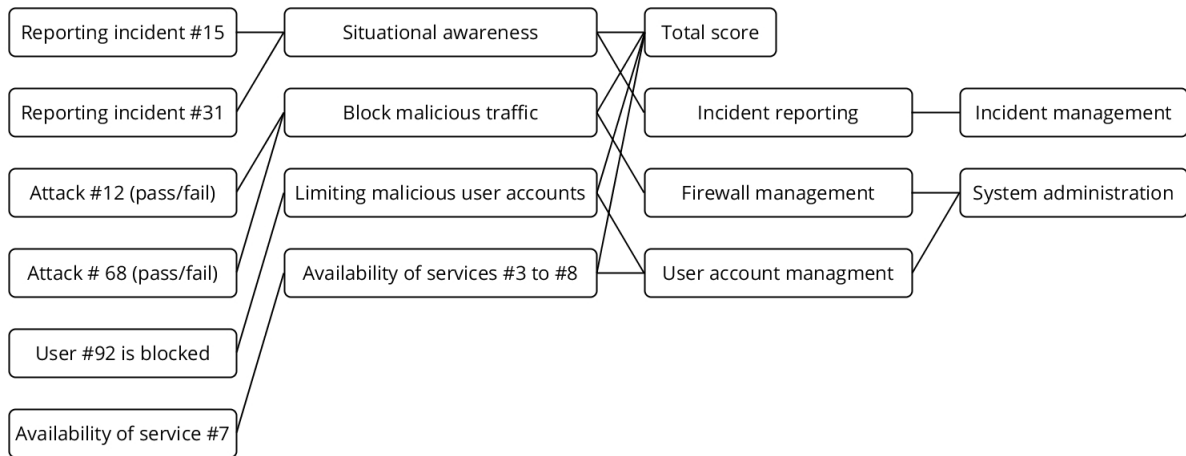


Figure 3: Sample of categorised performance metrics linked to skills

Figure 3 illustrates a mapping of performance metrics and skills in a hypothetical scenario. All the numbers (e.g. service #7) are arbitrary and for illustrative purposes only. There are six measurement points. Out of these, two measurement points are focusing on incident reporting. Those two give the input for the situational awareness category scoring. Optionally, the weight of reporting incident #15 and #31 could vary. For example, reporting incident #15 could be considered two times more important than reporting incident #31 and the weights could be set accordingly. Situational awareness together with the other performance metric categories gives input to the total score. In addition to being used for calculating the total score, it can be seen how situational awareness is used as an indication for the incident reporting skill. In the current example, the incident reporting skill is the only member of the incident management skill set. In reality, there can be numerous other skills that form together an input to the incident management skill set.

6. Future research

In this work, we defined metrics that are mostly based on common input sources such as the keyboard or the mouse. In the future, more inputs could be considered. Video feed from the in-built camera can be used to conduct eye tracking (Galdi *et al.*, 2016). Audio from the microphone can be analysed to measure user's stress level, group dynamics and emotional tonalities of the communication by voice (Shiva Prasad, Kodanda Ramaiah and Manjunatha, 2017). Keyboard input can be analysed further for purposes such as verifying the user identity (Bhattasali *et al.*, 2016).

Additionally, more research should be done regarding the dynamic analysis of serious game data. Cognitive principles for effective learning include creating learning scenarios that keep the participants in a zone between too easy and too difficult (Greitzer, Kuchar and Huston, 2007). Automatic analysis of performance metrics can allow the computerised serious game to adapt to individual needs of each participant and therefore provide a more engaging experience.

7. Conclusions

Serious games analytics (SEGA) is a growing field with diverse applicable implementations. We have identified computer science and cybersecurity as fitting areas to be linked with serious games analytics due to their extremely life-like VM-based simulation environments. To address the lack of systematic approach for connecting SEGA with VM-based serious games, we have outlined the main relevant performance metrics for measuring the skills of participants of VM-based serious games. The key measurement points are brought out together with their strengths and pitfalls. Furthermore, the approach for connecting between performance metric categories and skills is described.

In this paper, we have used cybersecurity related serious games as an example, but the same principles can be carried over to multiple other fields, especially to those that are connected to computer science.

8. Bibliography

- Alexandru Soceanu, Maksym Vasylenko and Alexandru Gradinaru (2017) 'Improving Cybersecurity Skills Using Network Security Virtual Labs', in *Proceedings of the International MultiConference of Engineers and Computer Scientists 2017 Vol II, IMECS*. Hong Kong. Available at: http://www.iaeng.org/publication/IMECS2017/IMECS2017_pp594-599.pdf (Accessed: 3 May 2017).
- Assante, M. J. and Tobey, D. H. (2011) 'Enhancing the Cybersecurity Workforce', *IT Professional*, 13(1), pp. 12–15. doi: 10.1109/MITP.2011.6.
- Bhattasali, T., Panasiuk, P., Saeed, K., Chaki, N. and Chaki, R. (2016) 'Modular logic of authentication using dynamic keystroke pattern analysis', *AIP Conference Proceedings*, 180012(101). doi: 10.1063/1.4951959.
- Buttyán, L., Félegyházi, M. and Pék, G. (2016) 'Mentoring talent in IT security – A case study', in *USENIX Workshop on Advances in Security Education (ASE '16)*. Available at: <https://www.usenix.org/system/files/conference/ase16/ase16-paper-butytyan.pdf> (Accessed: 2 May 2017).
- Cano, J., Hernandez, R., Ros, S. and Tobarra, L. (2016) 'A distributed laboratory architecture for game based learning in cybersecurity and critical infrastructures', in *2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV)*. IEEE, pp. 183–185. doi: 10.1109/REV.2016.7444461.
- Carlin, A. and Manson, D. (2011) 'A League of Our Own : The Future of Cyber Defense Competitions', *Communications of the IIMA*. International Information Management Association, 11(2), pp. 1–11. Available at: <http://scholarworks.lib.csusb.edu/ciima/vol11/iss2/1> (Accessed: 3 May 2017).
- DeRosier, M. E., Craig, A. B. and Sanchez, R. P. (2012) 'Zoo U : A Stealth Approach to Social Skills Assessment in Schools', *Advances in Human-Computer Interaction*. Hindawi Publishing Corp., 2012, pp. 1–7. doi: 10.1155/2012/654791.
- Djaouti, D., Alvarez, J. and Jessel, J.-P. (2011) 'Classifying serious games: The G/P/S model', *Handbook of research on improving learning and motivation through educational games: Multidisciplinary approaches*. IGI Global, (2005), pp. 118–136. doi: 10.4018/978-1-60960-495-0.ch006.
- Eck, R. Van (2006) 'Digital Game-Based Learning : It æ™ s Not Just the Digital Natives Who Are Restless', *Educause Review*. ACM, 41(2), pp. 1–16. doi: 10.1145/950566.950596.
- Ernits, M., Tammekänd, J. and Maennel, O. (2015) 'i-tee: A fully automated Cyber Defense Competition for Students', *ACM SIGCOMM Computer Communication Review*. ACM, 45(5), pp. 113–114. doi: 10.1145/2829988.2790033.
- Evans, K. & Reeder, R. (2010) *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters - A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Available at: www.csis.org (Accessed: 2 May 2017).
- Fernández-Sanz, L., Gómez-Pérez, J. and Castillo-Martínez, A. (2017) 'e-Skills Match: A framework for mapping and integrating the main skills, knowledge and competence standards and models for ICT occupations', *Computer Standards & Interfaces*, 51, pp. 30–42. doi: 10.1016/j.csi.2016.11.004.
- Furfaro, A., Argento, L., Parise, A. and Piccolo, A. (2017) 'Using virtual environments for the assessment of cybersecurity issues in IoT scenarios', *Simulation Modelling Practice and Theory*, 73, pp. 43–54. doi: 10.1016/j.simpat.2016.09.007.
- Galdi, C., Nappi, M., Riccio, D. and Wechsler, H. (2016) 'Eye movement analysis for human authentication: a critical survey', *Pattern Recognition Letters*, 84, pp. 272–283. doi: 10.1016/j.patrec.2016.11.002.
- Greitzer, F. L., Kuchar, O. A. and Huston, K. (2007) 'Cognitive science implications for enhancing training effectiveness in a serious gaming context', *Journal on Educational Resources in Computing*. ACM, 7(3), p. 2–es. doi: 10.1145/1281320.1281322.
- Hallaq, B., Nicholson, A., Smith, R., Maglaras, L., Janicke, H. and Jones, K. (2016) 'CYRAN: A Hybrid Cyber Range for Testing', in *Security Solutions and Applied Cryptography in Smart Grid Communications*. IGI Global, pp. 226–241. doi: 10.4018/978-1-5225-1829-7.ch012.
- Hays, R. T., Jacobs, J. W., Prince, C. and Salas, E. (1992) 'Flight simulator training effectiveness: A meta-analysis.', *Military Psychology*. Lawrence Erlbaum, 4(2), pp. 63–74. doi: 10.1207/s15327876mp0402_1.
- Henshel, D. S., Deckard, G. M., Lufkin, B., Buchler, N., Hoffman, B., Rajivan, P. and Collman, S. (2016) 'Predicting proficiency in cyber defense team exercises', in *MILCOM 2016 - 2016 IEEE Military Communications Conference*. IEEE, pp. 776–781. doi: 10.1109/MILCOM.2016.7795423.
- Jacobs, R., Beyer, E. and Carter, K. (2017) *Interprofessional simulation education designed to teach occupational therapy and nursing students complex patient transfers*, *Journal of Interprofessional Education & Practice*. doi: 10.1016/j.xjep.2016.12.002.
- Lateef, F. (2010) 'Simulation-based learning: Just like the real thing.', *Journal of emergencies, trauma, and shock*. Medknow Publications and Media Pvt. Ltd., 3(4), pp. 348–52. doi: 10.4103/0974-2700.70743.

- Ledford, H., Mountroudou, X. and Li, X. (2016) 'Denial of Service Lab for Experiential Cybersecurity Learning in Primarily Undergraduate Institutions', *Journal of Computing Sciences in Colleges*, 32(2), pp. 158–164. Available at: http://delivery.acm.org/10.1145/3020000/3015088/p158-ledford.pdf?ip=193.40.244.196&id=3015088&acc=PUBLIC&key=D2103A8F5527A3D9.5764A7F6B87355B6.4D4702B0C3E38B35.4D4702B0C3E38B35&CFID=757649657&CFTOKEN=70574058&__acm__=1493719799_5ff096bd9d26ea17fee04 (Accessed: 2 May 2017).
- Loeb, M. (2015) 'Cybersecurity talent: Worse than a skills shortage, it's a critical gap', *The Hill*, 17 April. Available at: <http://thehill.com/blogs/congress-blog/technology/239113-cybersecurity-talent-worse-than-a-skills-shortage-its-a>.
- Loh, C. S. and Sheng, Y. (2015) 'Measuring the (dis-)similarity between expert and novice behaviors as serious games analytics', *Education and Information Technologies*. Springer US, 20(1), pp. 5–19. doi: 10.1007/s10639-013-9263-y.
- Loh, C. S., Sheng, Y. and Ifenthaler, D. (2015) 'Serious Games Analytics: Theoretical Framework', in *Serious Games Analytics*. Cham: Springer International Publishing, pp. 3–29. doi: 10.1007/978-3-319-05834-4_1.
- Loh, C. S. and Yanyan Sheng (2013) 'Performance metrics for serious games: Will the (real) expert please step forward?', in *Proceedings of CGAMES'2013 USA*. IEEE, pp. 202–206. doi: 10.1109/CGames.2013.6632633.
- NATO CCDCOE (2017) *Locked Shields 2017*. Available at: <https://ccdcoe.org/locked-shields-2017.html> (Accessed: 2 May 2017).
- Newhouse, B., Keith, S., Scribner, B. and Witte, G. (2016) 'NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Education (NICE)', *Draft NIST Special Publication 800-181*. Available at: http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf (Accessed: 3 May 2017).
- Ottis, R. (2014) 'Light Weight Tabletop Exercise for Cybersecurity Education', *Journal of Homeland Security and Emergency Management*, 11(4), pp. 579–592. doi: 10.1515/jhsem-2014-0031.
- Shiva Prasad, K. M., Kodanda Ramaiah, G. N. and Manjunatha, M. B. (2017) 'Speech Features Extraction Techniques for Robust Emotional Speech Analysis/Recognition', *Indian Journal of Science and Technology*, 10(3). doi: 10.17485/ijst/2017/v10i3/110571.
- Starr, C. W., Manaris, B., Stalvey, R. H., Starr, C. W., Manaris, B. and Stalvey, R. H. (2008) 'Bloom's taxonomy revisited', *ACM SIGCSE Bulletin*. ACM, 40(1), p. 261. doi: 10.1145/1352322.1352227.
- Umbleja, K., Kuk, V., Jaanus, M. and Udal, A. (2014) 'New concepts of automatic answer evaluation in competence based learning', in *IEEE Global Engineering Education Conference, EDUCON*. IEEE, pp. 922–925. doi: 10.1109/EDUCON.2014.6826207.
- Wroclawski, J., Benz, T., Blythe, J., Faber, T., Hussain, A., Mirkovic, J. and Schwab, S. (2016) 'DETERLab and the DETER Project', in *The GENI Book*. Cham: Springer International Publishing, pp. 35–62. doi: 10.1007/978-3-319-33769-2_3.